

30 March 1972

PHYSICAL SECURITY

OF

REMOTE TERMINALS

BACKGROUND:

Physical security is certainly not a term that is new to any of us in government. It has, however, with the integration of the computer into our information systems taken on a more complicated and less clearly definable meaning. In fact, only in the last few years have commercial users and industry, with a few exceptions, begun to give physical security any real attention as they begin to move away from displaying their computer systems as "showplaces." Physical security can no longer be merely construed in terms of putting an approved lock on a door and ensuring that the walls run slab to slab. Sound physical control features or structures must be augmented with new and more practical innovations. Glass walls or partitions may not afford the protection of a concrete wall, but such a concrete wall prohibits visibility of the area from the outside and makes it possible for an intruder to do considerable damage before being detected. The luxury of building impenetrable fortresses is not available since cost factors of the new systems force us to ensure that each organization utilizes the full potential of the system. Because of the new considerations allowing for unvarying humidity ranges and immediate response in the event of fire, physical security cannot just protect the installation, it also must now participate in maintaining the system.

It is difficult to make sound determinations of the need for security measures or to justify not applying them unless there is a quantitative assessment of the value of the data being protected.

Physical security plays an integral part in protecting the classified, compartmented, or otherwise privileged data in an information system against access by persons not cleared for and/or not authorized access to that data. No information system can be absolutely secure, however, every reasonable effort must be taken to ensure that the probability of compromise is severely minimized. Consequently, the physical security standards applied to every "link" or access point to the system itself must be commensurate with the highest level of the information in the system.

With the "expansion" of the computer center to remote terminals, we have, in fact, significantly increased the potential threat to subvert the system. The remote terminal cannot be allowed to become the "weak link" in the security chain. Such immediate factors as emanations, intrusion, and physical access control measures must be considered in the overall planning of the physical protection of each remote terminal. While at the same time, conscious of electronic eavesdropping and that, by observing the terminal in operation or by collecting the discarded printouts or printing ribbons, a person could possibly gain the necessary passwords to allow him unauthorized access to the files and programs of all or part of the information system. Without applying the same stringent physical standards at each terminal the relatively elaborate measures taken to protect the entire information system itself becomes sharply devalued.

Incidental to these purposes is the need to prevent damage to facilities and equipment at the terminal due to accidents, disasters, or acts of sabotage.

PROBLEMS:

In the foregoing section this paper alluded to a number of problems concerning remote terminals. Some of the more significant areas of concern facing an organization about to implement such a system are:

1. The actual physical location of the building; that is to say, is the location in an isolated area, public area?
2. The peripheral security measures that encompass this building; such as fences, hedges, etc. Included in this section are exterior guard patrol.
3. Access control measures implemented in an agency or building; this includes internal guards, who must have a clearly defined role and instructions in the event of unauthorized entry or disruptions.
4. Specific location of the remote terminal area; included in this category are again access controls, since this type of area will be designed a secure or restricted area because of the direct link into the computer center (data base).
5. Locking devices, ultrasonic alarms - which type and model should be installed and where.
6. Disaster control procedures including fire, water, and riot control measures.

ANSWERS:

In this concept of remote terminals physical security measures are the initial barrier for the protection of such devices. These measures are interwoven into the overall hardware and software security procedures. The following are suggested applications which are generally accepted throughout the intelligence/security community:

1. Adequate guard force with a concise pass system for employees identification and the installation itself must afford a significant deterrent to the entry of unauthorized persons.
2. Define security or restricted area, conduct liaison and coordination with involved offices to arrive at an approved plan.
3. Separate identification for users of the remote terminal and a strict enforcement of the "need to know" doctrine.
4. Eliminate all unnecessary traffic throughout remote terminal area and prominent signs that identify the location of the terminal inviting unnecessary attention.
5. Restrict access to the remote terminal to authorized operating personnel and supervisory personnel. This number should be kept to an absolute minimum and their duties and responsibilities must be clearly defined.
6. Implement remote terminal access logs with employees including requirement that they log in and out.
7. Visitors should be given appropriate identification badges and escort.

CONCLUSION:

While the foregoing may be the panacea for physical security problems, failure to test security measures can easily result in a reliance on a number of things which are ineffective. Reasonably frequent tests of security measures indicate a continuing awareness and concern for security and for that reason, are in themselves a security measure in that they improve the sensitivity of employees toward security as a continuing problem.

Clearly conceived and normally effective security measures become quite ineffective when people find they can circumvent them without incurring punitive action.